Computer Networks

Dr. Ali Sayyed
Department of Computer Science
National University of Computer & Emerging Sciences

Link Access

- *Random Access Protocols*
- *Taking Turn Protocols*

Introduction

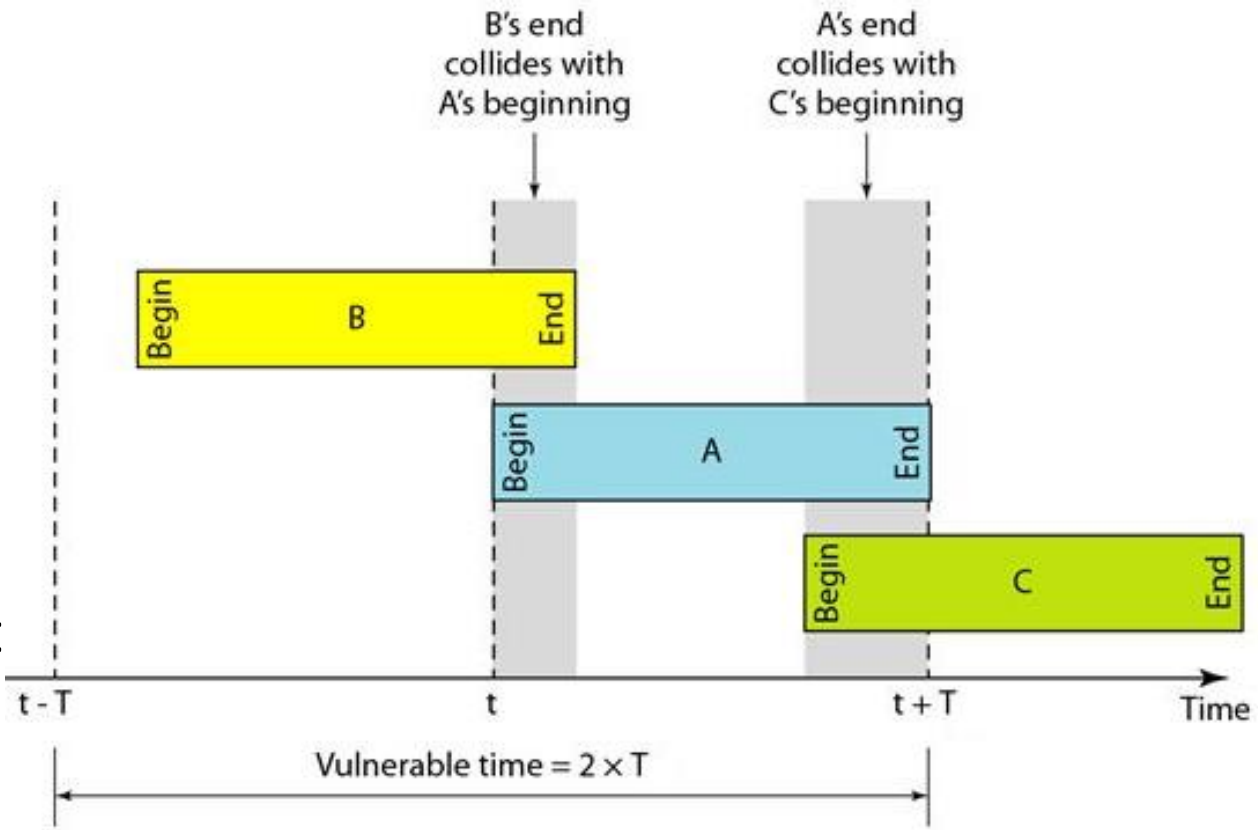
- In Random access protocols, each device has an equal privilege to access the network and transmit data. These protocols allow nodes to send and receive data without taking turns or waiting for permission.
- A transmitting node transmits.
  - In case of a collision, repeatedly retransmits its frame until it gets through without a collision.
  - However, it doesn't necessarily retransmit the frame right away. Instead, it waits a random delay before retransmitting .
- It is possible that one of the nodes will pick a random delay that is sufficiently less than the delays of the other colliding nodes and will therefore be able to send its frame.

Pure ALOHA

- ALOHA is an early Random Access protocol.
- In pure ALOHA, Whenever a station has a data, it transmits i.e. frames are transmitted at completely arbitrary times.
- If two or more devices transmit simultaneously, their messages will collide and be corrupted
- If acknowledgement is not received within specified time, the sender assumes that the frame has been lost.
- The sender waits for a random amount of time and sends the frame again.
- This waiting time must be random otherwise same frames will collide again and again.

Pure ALOHA

- Each transmitted packet in pure ALOHA is vulnerable to collisions
  - Let all frames have same length and have transmission time = T
  - Suppose frame A is sent at time t
  - If frame B sent at any time between t– T and t, collision will occur.
  - If frame C sent any time between t and t+ T, collision will occur.
- So, total vulnerable time for frame A is 2T

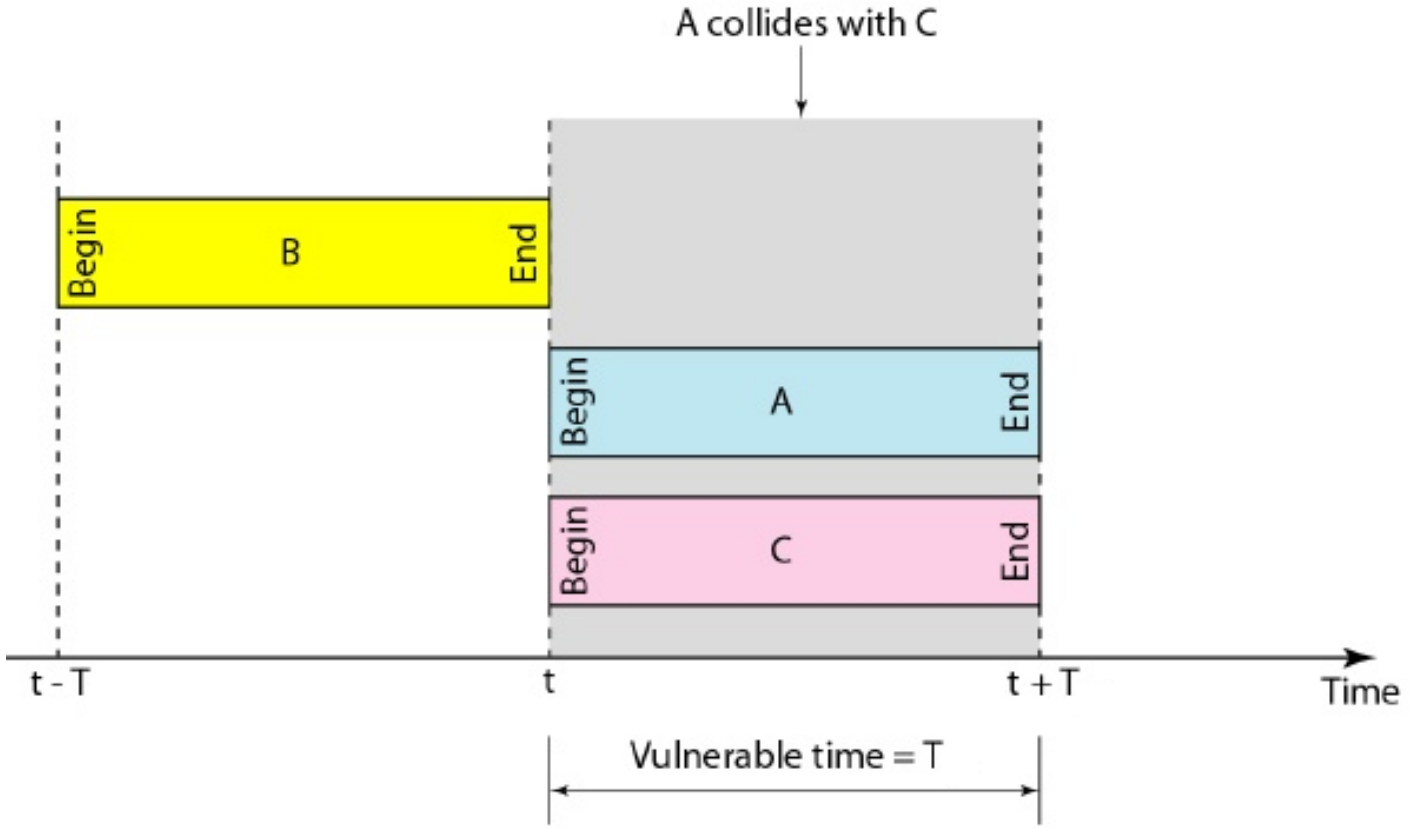


Slotted ALOHA

- Can increase efficiency of ALOHA using slotted time system
- Time is divided into fixed slots, each slot equal to frame Tx time
- All users synchronized to these time slots
  - Frames are transmitted only in the beginning of a slot
  - Frames held until next time slot for transmission if generated in-between transmission slots
  - Synchronization achieved by transmitting periodic synch pulses from one designated station in the network

Slotted ALOHA

- Vulnerable period reduced to T



CSMA-CA (Carrier Sense Multiple Access – Collision Avoidance)

- **Listen before speaking**.
  - If someone else is speaking, wait until they are finished.
  - In the networking world, this is called ***carrier sensing***—a node listens to the channel before transmitting. If there is an ongoing transmission, wait until that transmissions is over and then begins transmission.
- Hence, it reduces the chances of a collision on a transmission medium.

Carrier Sensing Methods

- **Persistent method**
  - If the medium is not idle, continuously sense the medium.
  - Still there is a chance of collision

- **Nonpersistent method**
  - If the medium is not idle, wait a random amount time and then senses again
  - Reduces collision, reduce network efficiency

p-persistent CSMA

- Node listens to channel to determine if the channel is idle or busy
- If channel is busy, node listens continuously, waiting until the channel becomes free
- Once channel is free, node sends the frame with probability p
- **Strategy:** transmit packet with Pr = p when channel is free
- Node waits for an ACK
- If no ACK received, node waits a random amount of time and resumes listening to the channel
- When channel again sensed idle, frame retransmitted with probability p

p-persistent CSMA

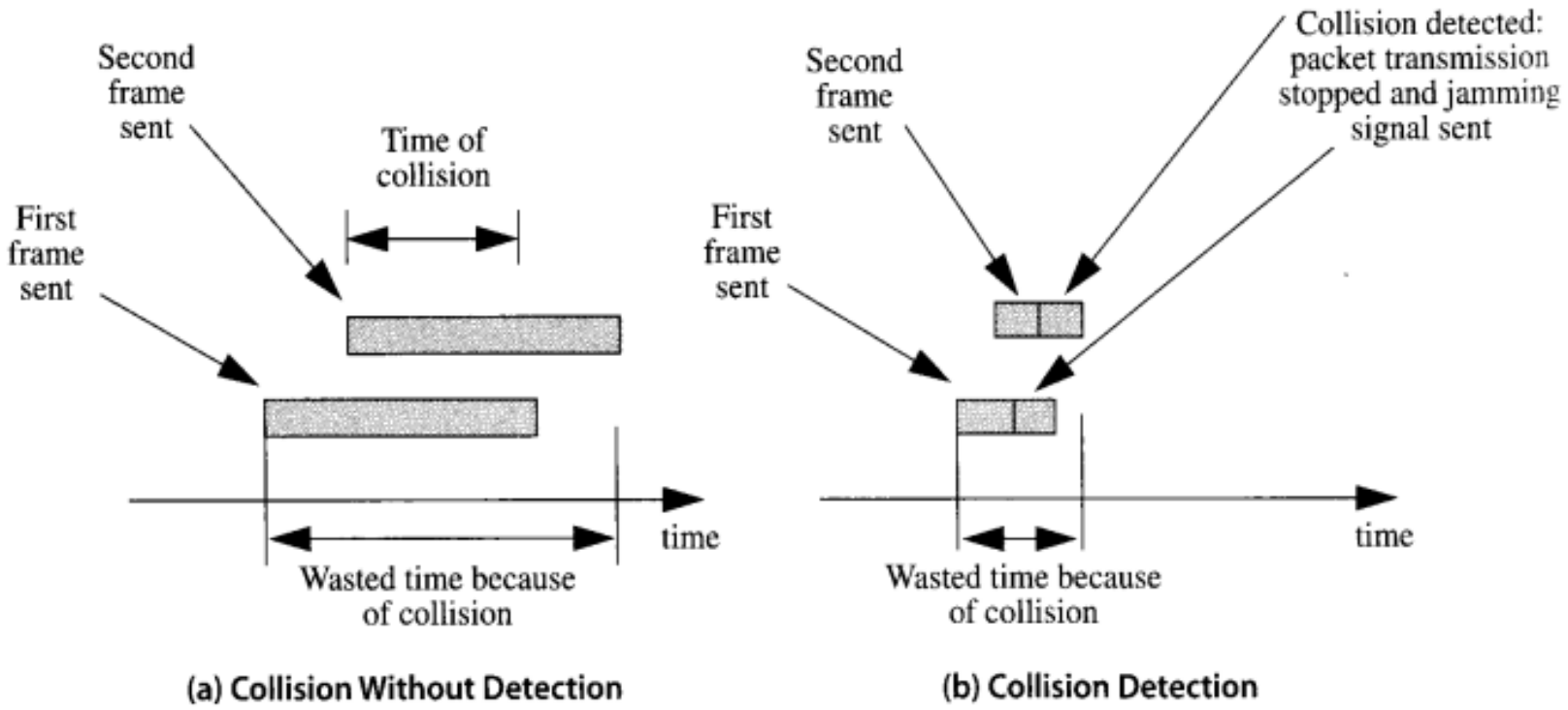
- Collisions can occur
  - **Propagation delays:** Node A might sense idle channel even though Node B already began transmitting
  - If Node A and Node B are sensing a busy channel at the same time, as soon as the channel is free, **both A and B will begin transmitting** their data
- Throughput performance much better than ALOHA
- **Slotted p-persistant CSMA** where nodes begin transmission at the beginning of time slots
- If p = 1, we call it **1-persistent CSMA**, which means it always transmits when the medium is quiet.

Nonpersistent CSMA

- Node listens to channel (perform carrier sensing)
  - If channel idle, node transmits data
  - Otherwise, node again waits a randomly selected interval of time before sensing again
- Randomized waiting times between channel sensing eliminate most collisions resulting from multiple users transmitting simultaneously upon sensing the transition from busy to idle
- This approach is **good at high traffic loads**
- Again we have a Slotted version of nonpersistent CSMA

Collision Detection

- What if we monitor the medium to listen for collisions too!



CSMA/CD

- **If someone else begins talking at the same time, stop talking**.
  - In the networking world, this is called ***collision detection***—a transmitting node listens to the channel while it is transmitting. If it detects that another node is transmitting, it stops transmitting and waits a random amount of time before repeating the same steps.

CSMA/CD

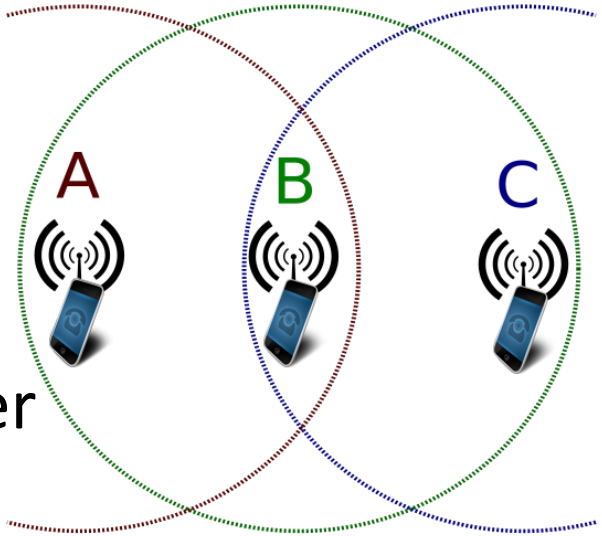
- **Carrier Sense Multiple Access with Collision Detection**
- To send a frame, listens to the medium to see if it is busy.
- If the medium is busy, it waits.
- If the station is able to transmit a frame, it listens to the medium for collision while transmitting the frame.
- If it detects a collision, it immediately stops the transmission and sends a short jamming signal.
- If it receives a jamming signal, it stops the transmission immediately.
- After a collision, it waits a random amount of time and then repeats the above steps.

Location-Dependent Carrier Sensing

- Carrier Sensing depends on location of the node
  - Transmitter performs Carrier Sensing
  - Know the state of the channel at transmitter
  - Cannot determine the state of the channel at the receiver
- Causes two problems
  - Hidden Nodes
  - Exposed Nodes

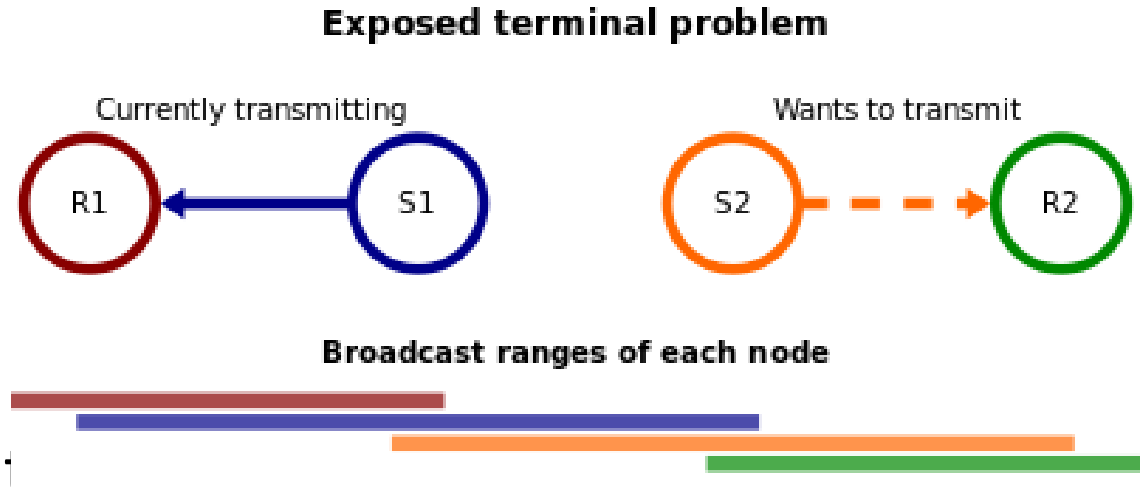
Hidden Terminal Problem

- A node that is within range of the receiver but not in range of the transmitter
- A hidden node will sense an idle channel and transmit data
  - Suppose node A is transmitting to node B
  - Node C will sense the channel as idle
    - Since A is outside the range of node C
    - C will transmit data to B, and will causes collision
- **Problem:** collisions is actually detected at the transmitter but it can also occur at the receiver
- Nodes outside the range of the transmitter "hidden" to the transmitter so CSMA not effective



Exposed Nodes

- A node that is within range of the sender but out of range of the receiver
- An exposed node will sense a busy channel and not transmit
  - Suppose S1 is transmitting to R1
  - S2 will sense a busy channel
  - However, S2 could transmit to R2
    - R2 is outside the range of R1
    - No collision
  - S2 is prevented from transmitting to R2
  - Causes underutilization of the channel



Handshaking Mechanism - MACA

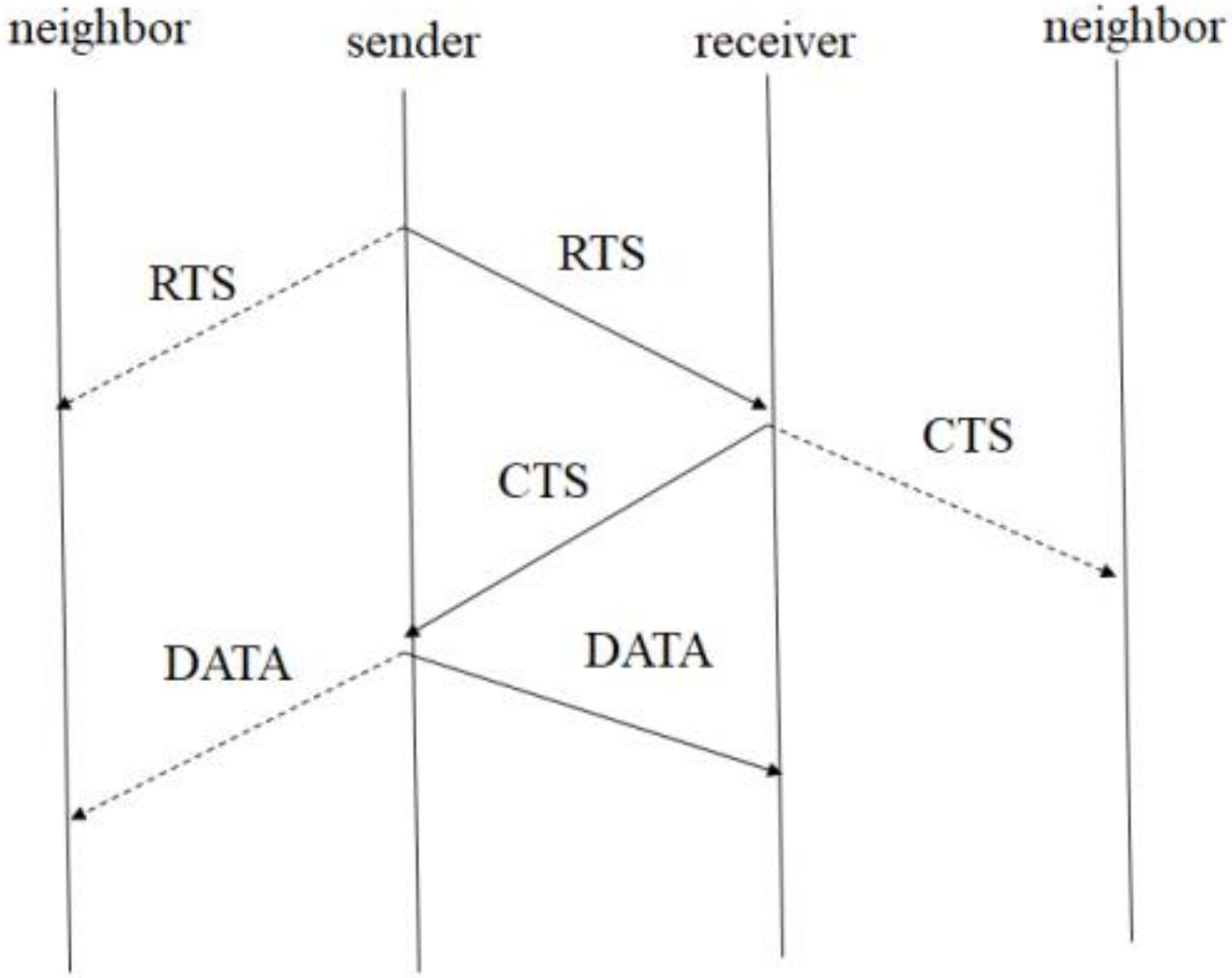
- MACA implements hand-shaking collision avoidance
  - Precede data transmission with request-to-send (RTS) packet
    - RTS contains length of expected data transmission
    - All nodes in vicinity of Tx node enter backoff (become silent) for duration of message delivery
  - If Rx node receives RTS, replies with a clear-to-send (CTS) packet
    - CTS packet contains length of expected data transmission
    - All nodes in vicinity of Rx node enter backoff (become silent) for duration of message delivery
  - Upon receipt of CTS, Tx node sends data

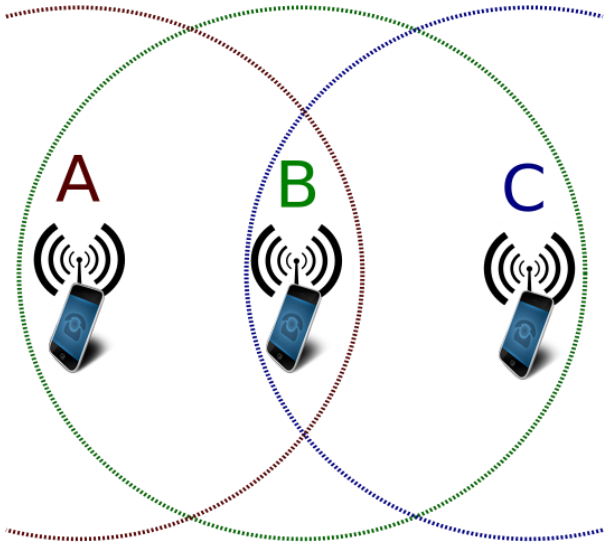
Handshaking Mechanism - MACA

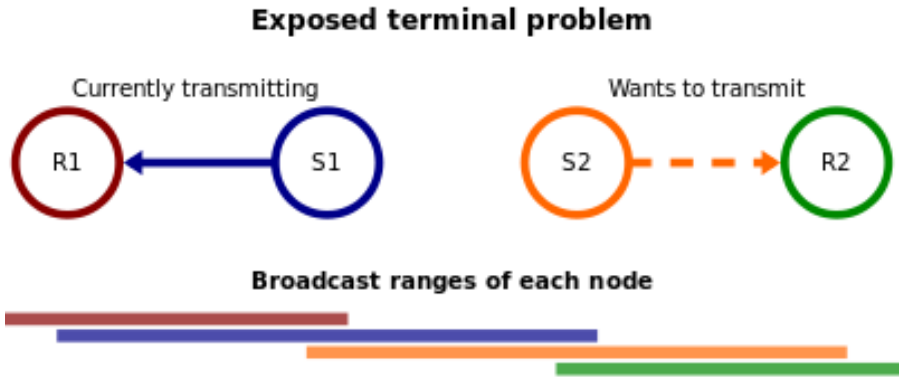
- MACA successfully alleviates the hidden terminal and exposed terminal problems
  - All nodes, that could corrupt transmission (any nodes hearing CTS), do not transmit – **virtual carrier sense**
    - **Hidden Nodes**
  - All nodes that would not corrupt transmission (any nodes only hearing RTS and not CTS), can transmit without corrupting communication between Rx and Tx
    - **Exposed Nodes**

Please see an animation at *https://www2.tkn.tu-berlin.de/teaching/rn/animations/csma/*

Packet Transmission in MACA







Taking Turn Protocols

Polling Protocol

- The polling protocol requires one of the nodes to be designated as a Master node.
- The Master node “invites” slave nodes to transmit in turn.
- In particular, the master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum number of frames.
- After node 1 transmits some frames, the master node tells node 2 it (node 2) can transmit up to the maximum number of frames.
  - The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel.
- The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.

Polling Protocol

- The polling protocol eliminates the collisions and empty slots that plague random access protocols. This allows polling to achieve a much higher efficiency.
- But it also has a few drawbacks.
  - The first drawback is that the protocol introduces a polling delay—the amount of time required to notify a node that it can transmit.
  - The second drawback, which is potentially more serious, is that if the master node fails, the entire channel becomes inoperative. The 802.15 protocol and the Bluetooth protocol re examples of polling protocols

Token-passing Protocol

- In this protocol there is no master node.
- The stations are organized into a logical ring.
- A small, special-purpose frame known as a token is exchanged among the nodes in some order.
- A station can transmit data only when it has the token frame.
- When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node. If a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node.

Token-passing Protocol

- Token passing is decentralized and highly efficient.
- But it has its problems as well.
- For example, the failure of one node can crash the entire channel.
- Or if a node accidentally neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation.
- Over the years many token-passing protocols have been developed, including the
  - fiber distributed data interface (FDDI) protocol and
  - the IEEE 802.5 token ring protocol [IEEE 802.5 2012]